IFIP Advances in Information and Communication Technology 484

Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the first World Computer Congress held in Paris the previous year. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

> *IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.*

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is generally smaller and occasionally by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at http://www.springer.com/series/6102

Gilbert Peterson · Sujeet Shenoi (Eds.)

Advances in Digital Forensics XII

12th IFIP WG 11.9 International Conference,
New Delhi, January 4–6, 2016
Revised Selected Papers

Springer

Editors
Gilbert Peterson
Department of Electrical and Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, Ohio
USA

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa
Tulsa, Oklahoma
USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-46278-3 ISBN 978-3-319-46279-0 (eBook)
DOI 10.1007/978-3-319-46279-0

Library of Congress Control Number: 2016950753

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Contents

Contributing Authors

Oluwapelumi Aboluwarin is a Software Engineer with Nexmo, London, United Kingdom. His research interests include natural language processing, text mining and conversational user interfaces.

Sudhir Aggarwal is a Professor of Computer Science at Florida State University, Tallahassee, Florida. His research interests include password cracking, information security and building software tools and systems for digital forensics.

Irfan Ahmed is an Assistant Professor of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests are in the areas of malware detection and analysis, digital forensics, industrial control systems security and Internet of Things security.

Ahmed Almarzooqi is a Ph.D. student in Digital Forensics at De Montfort University, Leicester, United Kingdom. His research interests include digital forensics and information security.

Panagiotis Andriotis is a Research Associate in the Information Security Research Group, Department of Computer Science, University College London, London, United Kingdom. His research interests include digital forensics, text mining, content analysis, systems security and human aspects of security, privacy and trust.

Sara Baghbanzadeh is a Software Engineer with Gnowit, Ottawa, Canada. Her research interests include web crawling and session reconstruction for rich Internet applications.

Andres Barreto is a Software Developer for Archon Information Systems, New Orleans, Louisiana. His research interests include digital forensics and building scalable and usable web applications.

Nicole Beebe is an Associate Professor of Cyber Security at the University of Texas at San Antonio, San Antonio, Texas. Her research interests include digital forensics, cyber security and advanced analytics.

Gregor Bochmann is a Professor of Computer Science at the University of Ottawa, Ottawa, Canada. His research interests include software engineering for distributed applications, peer-to-peer systems and rich Internet applications.

Mikhaila Burgess is an Associate Professor of Digital Forensics at Noroff University College, Kristiansand, Norway. Her research interests include digital forensics, information security, data management and big data.

Raymond Chan is a Ph.D. student in Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics and critical infrastructure protection.

Vivien Chan is a Research Project Manager at the University of Hong Kong, Hong Kong, China. Her research interests include cyber criminal profiling and digital forensics.

Kam-Pui Chow is an Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include information security, digital forensics, live system forensics and digital surveillance.

Swasti Bhushan Deb is a Senior Project Manager at the Kolkata Cyber Laboratory, Data Security Council of India, Kolkata, India. His research interests include cyber crime detection, and computer and mobile device forensics.

Muhammad Faheem is a Post-Doctoral Researcher in the Department of Computer Science at the University of Ottawa, Ottawa, Canada. His research interests include information retrieval, web archiving, knowledge representation logics and rich Internet applications.

Jayaprakash Govindaraj is a Senior Technology Architect at Infosys, Bangalore, India; and a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include mobile device security, digital forensics, web application security, Internet of Things security and security in emerging technologies.

Gaurav Gupta is a Scientist D in the Department of Electronics and Information Technology, Ministry of Information Technology, New Delhi, India. His research interests include digitized document fraud detection, mobile device forensics and cloud forensics.

Salman Hooshmand is a Ph.D. candidate in Computer Science at the University of Ottawa, Ottawa, Canada. His research interests include software engineering and rich Internet applications modeling and testing.

Andrew Jones is a Professor of Cyber Security and Digital Forensics and Director of the Cyber Security Centre at the University of Hertfordshire, Hatfield, United Kingdom. His research interests include digital forensics, information security and risk management.

Guy-Vincent Jourdan is a Professor of Computer Science at the University of Ottawa, Ottawa, Canada. His research interests include distributed systems modeling and analysis, formal system testing, rich Internet applications and software security.

Umit Karabiyik is an Assistant Professor of Computer Science at Sam Houston State University, Huntsville, Texas. His research interests include digital forensics, cyber security, computer and network security, and expert systems.

Rajesh Kumar is an Assistant Professor of Forensic Science at the Institute of Forensic Science, Aurangabad, India. His research interests include computational forensics, multimedia forensics, image processing and pattern recognition.

Michael Kwan is an Honorary Associate Professor of Computer Science at the University of Hong Kong, Hong Kong, China. His research interests include digital forensics and cyber investigations.

Changwei Liu is a Researcher in the Department of Computer Science at George Mason University, Fairfax, Virginia. Her research interests include cyber security and network forensics.

Huiming Liu is an M.S. student in Computer Science at Tsinghua University, Beijing, China. His research interests include network and mobile device security.

Lishu Liu is a Machine Learning Engineer at RetailMeNot, Austin, Texas. Her research interests involve the application of machine learning algorithms to locate, extract and present relevant information from massive data sets.

Wei Liu is an M.S. student in Computer Science at Tsinghua University, Beijing, China. His research interests include network and mobile device security.

Seyed Mirtaheri is a Research Assistant in the Department of Computer Science at the University of Ottawa, Ottawa, Canada. His research interests include parallel processing, distributed systems, web crawling and rich Internet applications.

Martin Olivier is a Professor of Computer Science at the University of Pretoria, Pretoria, South Africa. His research focuses on digital forensics – in particular the science of digital forensics and database forensics.

Iosif Viorel Onut is a Principal R&D Strategist at the Center for Advanced Studies, IBM Canada Lab, Ottawa, Canada; and an Adjunct Professor of Computer Science at the University of Ottawa, Ottawa, Canada. His research interests include software security, rich Internet applications and information security.

Sriram Raghavan is a Forensic Data Scientist with Telstra in Melbourne, Australia; and a Visitor in the Department of Computing at the University of Melbourne, Melbourne, Australia. His research interests include the development of quantitative metrics for cyber security and the mathematical foundations of security incident analysis.

S.V. Raghavan is the Chief Architect of India's National Knowledge Network in New Delhi, India; and a retired Professor of Computer Science and Engineering at the Indian Institute of Technology Madras, Chennai, India. His research interests include the design of scalable, large-scale secure networks.

Huw Read is an Associate Professor of Digital Forensics and Director of the Center for Advanced Computing and Digital Forensics at Norwich University, Northfield, Vermont. His research interests include digital forensics and computer security.

Vassil Roussev is a Professor of Computer Science at the University of New Orleans, New Orleans, Louisiana. His research interests include digital forensics, cyber security, distributed systems and human-computer interaction.

Ravi Saharan is an Assistant Professor of Computer Science and Engineering at the Central University of Rajasthan, Ajmer, India. His research interests include algorithms, computer graphics, image processing and steganography.

Bhupendra Singh is a Ph.D. student in Computer Science and Engineering at the Defence Institute of Advanced Technology, Pune, India. His research interests include digital forensics, file system analysis and user activity analysis on Windows systems.

Anoop Singhal is a Senior Computer Scientist in the Computer Security Division at the National Institute of Standards and Technology, Gaithersburg, Maryland. His research interests include network security, network forensics, web services security and data mining systems.

Gaurav Somani is an Assistant Professor of Computer Science and Engineering at the Central University of Rajasthan, Ajmer, India. His research interests include distributed systems, computer networks, cloud computing and digital forensics.

Minghe Sun is a Professor of Management Science and Statistics at the University of Texas at San Antonio, San Antonio, Texas. His research interests include mathematical programming and related areas for classification and solving hard optimization problems.

Iain Sutherland is a Professor of Digital Forensics at Noroff University College, Kristiansand, Norway. His research interests include digital forensics and data recovery.

Atsuhiro Takasu is a Professor in the Digital Content and Media Services Research Division at the National Institute of Informatics, Tokyo, Japan. His research interests include symbol sequence and time series analysis based on statistical models and their application to information integration.

Songpon Teerakanok is an M.S. student in Information Science and Engineering at Ritsumeikan University, Shiga, Japan. His research interests include cryptography, location-based services, privacy and digital forensics.

Elizabeth Thomas is a Consultant at Coalfire Systems, Manchester, United Kingdom. Her research interests include digital forensics and payment card systems.

Theo Tryfonas is a Senior Lecturer in Systems Engineering at the University of Bristol, Bristol, United Kingdom. His research interests are in the areas of smart cities, cyber security, systems engineering and technologies for sustainable development.

Tetsutaro Uehara is a Professor of Information Science and Engineering at Ritsumeikan University, Shiga, Japan. His research interests include digital forensics, cyber security and information system management.

Robin Verma is a Ph.D. student in Computer Science and Engineering at Indraprastha Institute of Information Technology, New Delhi, India. His research interests include digital forensics, privacy-enhancing technologies and mobile device forensics.

Duminda Wijesekera is a Professor of Computer Science at George Mason University, Fairfax, Virginia. His research interests include systems security, digital forensics and transportation systems.

Konstantinos Xynos is the Computer Security Course Leader at the University of South Wales, Pontypridd, United Kingdom. His research interests include computer security, computer forensics, network security and reverse engineering.

Haiyu Yang is an M.S. student in Thermal Engineering and a visiting graduate student in the Network and Information Security Laboratory at Tsinghua University, Beijing, China. His research interests include mobile device forensics and systems security.

Jianwei Zhuge is an Associate Professor of Computer Science in the Institute for Network Science and Cyberspace at Tsinghua University, Beijing, China. His research interests include Internet threat detection, malware analysis, and software vulnerability analysis and mitigation.

Preface

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every type of crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in information assurance – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems.

This book, *Advances in Digital Forensics XII*, is the twelfth volume in the annual series produced by the IFIP Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book presents original research results and innovative applications in digital forensics. Also, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

This volume contains twenty revised and edited chapters based on papers presented at the Twelfth IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India on January 4-6, 2016. The papers were refereed by members of IFIP Working Group 11.9 and other internationally-recognized experts in digital forensics. The post-conference manuscripts submitted by the authors were rewritten to accommodate the suggestions provided by the conference attendees. They were subsequently revised by the editors to produce the final chapters published in this volume.

The chapters are organized into eight sections: Themes and Issues, Mobile Device Forensics, Network Forensics, Cloud Forensics, Social Media Forensics, Image Forensics, Forensic Techniques, and Forensic Tools. The coverage of topics highlights the richness and vitality of the discipline, and offers promising avenues for future research in digital forensics.

This book is the result of the combined efforts of several individuals. In particular, we thank Gaurav Gupta, Robin Verma and Jayaprakash Govindaraj for their tireless work on behalf of IFIP Working Group 11.9. We also acknowledge the support provided by the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India; U.S. National Science Foundation; U.S. National Security Agency; and U.S. Secret Service.

Gilbert Peterson and Sujeet Shenoi